Background

Identify valid email-accounts.

Pre-requisites

Risks

Depending on the lockout policy you risk locking out users, and thus cause considerable damage.

It also produces lots of logs.

How to check for

First check if the accounts is valid. https://github.com/LMGsec/o365creeper

Perform password spraying attack: https://github.com/dafthack/MailSniper

How to exploit

Recommendation

Related Vulnerabilities

This finding should not be reported as the name of this issue, instead it should be reported as the vulnerabilities written below. The below written vulnerabilities map to the vulnerability-descriptions in that repo.

For example, if kerberoast, report as the following vulnerabilities if they are applicable:

- Weak password [ID of issue]
- Overpriviliged kerberoastable user [ID of issue]

References

https://github.com/LMGsec/o365creeper